02:00:00

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION
- - -

UNITED STATES OF AMERICA,	:	CASE NO. 1:18-cr-0043
	:	
Plaintiff,	:	
vs.	:	TRIAL EXCERPT
	:	
YANJUN XU, also known as XU	:	26th of OCTOBER, 2021
YANJUN, also known as QU HUI,	:	3:18 P.M.
also known as ZHANG HUI,	:	
	:	
Defendant.	:	

- - -

EXCERPT OF TRANSCRIPT OF PROCEEDINGS
TESTIMONY OF ADAM ROBERT JAMES
BEFORE THE HONORABLE TIMOTHY S. BLACK, JUDGE
- - -

APPEARANCES:

For the Plaintiff:

Timothy S. Mangan, Esq.
Emily N. Glatfelter, Esq.
Assistant United States Attorneys
221 East Fourth Street, Suite 400
Cincinnati, Ohio 45202
and
Matthew John McKenzie, Esq.
United States Department of Justice
National Security Division
950 Pennsylvania Avenue NW
Washington, D.C. 20530
and
Jacqueline K. Prim
Special Assistant, Paralegal
United States Department of Justice
National Security Division
950 Pennsylvania Avenue NW
Washington, D.C. 20530

For the Defendant:

Ralph William Kohnen, Esq.
Jeanne Marie Cors, Esq.
Sanna-Rae Taylor, Esq.
Taft Stettinius and Hollister
425 East Walnut Street, Suite 1800
Cincinnati, Ohio 45202
and

Robert K. McBride, Esq.
Amanda Johnson, Esq.
Taft Stettinius and Hollister
50 East RiverCenter Boulevard
Suite 850
Covington, Kentucky 41011
and
Florian Miedel, Esq.
Miedel & Mysliwiec, LLP
80 Broad Street, Suite 1900
New York, New York 10004

Also present: Mae Harmon, Interpreter
Robin Murphy, Interpreter
Yanjun Xu, Defendant

Law Clerk: Cristina V. Frankian, Esq.

Courtroom Deputy: Rebecca Santoro

Stenographer: Mary Schweinhagen, RPR, RMR, RDR, CRR
United States District Court
200 West Second Street, Room 910
Dayton, Ohio 45402

Proceedings reported by mechanical stenography, transcript produced by computer.

*** *** *** ***

INDEX OF WITNESSES

TUESDAY, OCTOBER 26, 2021

	DIRECT	CROSS	REDIRECT	RECROSS
PLAINTIFF'S WITNESSES				
ADAM JAMES	5			

*   *   *   *   *

P-R-O-C-E-E-D-I-N-G-S 3:18 P.M.

(Proceedings reported but not transcribed.)

03:18:26 MR. McKENZIE: Your Honor, the government is ready
03:18:27 to call our next witness, Special Agent Adam James.

03:18:31 THE COURT: Very well. If we could call for the
03:18:33 agent, special agent.

03:18:37 MS. TAYLOR: Your Honor, counsel for --

03:18:38 THE COURT: Yes?

03:18:39 MS. TAYLOR: Counsel for defense is going to change
03:18:43 places at the tables.

03:18:43 THE COURT: Change what?

03:18:43 MS. TAYLOR: Change places at the tables if that's
03:18:44 okay?

03:18:45 THE COURT: Yes.

03:18:45 MS. TAYLOR: Thank you.

03:19:02 THE COURT: If the witness would be willing to
03:19:03 approach, we're going to put you in the witness stand over
03:19:06 here.

03:19:10 If you'd be willing to pause for the oath to tell the
03:19:13 truth. If you'd raise your right hand. Do you solemnly swear
03:19:16 or affirm that your testimony today will be the truth, subject
03:19:21 to penalty of perjury?

03:19:23 THE WITNESS: I do.

03:19:24 THE COURT: Very well. Once you get seated, get
03:19:27 close to the microphone.

03:19:30 The lawyer for the government may begin with questions.

03:19:30 **ADAM ROBERT JAMES, PLAINTIFF WITNESS, SWORN**

03:19:33 **DIRECT EXAMINATION**

03:19:33 BY MR. McKENZIE:

03:19:34 **Q.** Good afternoon. My name is Matthew McKenzie.

03:19:38 Will you please state your full name and spell your last
03:19:40 name for the record?

03:19:41 **A.** My name is Adam Robert James, J-A-M-E-S.

03:19:49 **Q.** By whom are you employed?

03:19:51 **A.** The FBI.

03:19:53 **Q.** To which field office are you assigned?

03:19:58 **A.** I'm assigned to the San Diego field office.

03:20:02 **Q.** What is your current position within the FBI?

03:20:06 **A.** I am a special agent.

03:20:09 **Q.** How long have you been a special agent?

03:20:11 **A.** I became a special agent on July 5th of 2010.

03:20:17 **Q.** Do you have a particular focus?

03:20:21 **A.** Yes. I'm focused on cyber crime investigations.

03:20:24 **Q.** What types of activities are included in cyber crime?

03:20:30 **A.** There's various types of cyber crime that the FBI
03:20:33 investigates. It could be ransomware. It could be business
03:20:39 email compromises. But I mainly focus on computer intrusion
03:20:43 activity.

03:20:45 **Q.** Has the FBI provided you with any training regarding
03:20:50 computer intrusions and cyber investigations?

03:20:53 **A.** Yes, it has.
03:20:54 **Q.** Could you provide the jury with an overview of your
03:20:59 training that was provided by the FBI?
03:21:01 **A.** Yes. So when you get hired by the FBI, they send you
03:21:05 to the FBI Academy for about five months for general
03:21:08 training. That covers a little bit of cyber crime training,
03:21:12 but very little.
03:21:13 When you get assigned to a cyber squad once you get out
03:21:17 of the academy, they send you to additional training. So
03:21:20 the first training I took was a two-week general cyber
03:21:25 investigation course where they kind of tell you here's all
03:21:29 the elements of the FBI that does cyber crime
03:21:33 investigations, and then they give you kind of like a brief
03:21:37 week-long course in cyber investigations.
03:21:40 And then since then I have taken over 400 hours of
03:21:43 training both online and in person. That has included
03:21:47 everything from interview and interrogation techniques;
03:21:51 hacker tactics, techniques, and procedures; reverse
03:21:55 engineering malware; and computer forensics; and intrusion
03:21:59 investigations.
03:21:59 **Q.** We'll come back and define some of those terms in a
03:22:03 moment. But prior to joining the FBI, where did you work?
03:22:10 **A.** Immediately prior to joining the FBI, I worked for a
03:22:15 computer security consulting company in Omaha, Nebraska.
03:22:17 **Q.** And what were some of your duties and responsibilities?

03:22:19 **A.** My primary duty immediately before joining the FBI was computer forensics and incident response. Prior to that I did some third-party risk assessments and policy writing for various companies.

03:22:35 **Q.** Did you ever -- in that capacity as a consultant, did you ever contract with the U.S. government?

03:22:42 **A.** I took a -- about a nine-month leave of absence from my job with the consulting company, and I did media forensics for a U.S. military in Iraq.

03:22:58 **Q.** Will you just explain to the jury in basic terms what you did over in Iraq?

03:23:05 **A.** Yeah. So basically what my job was, is when the military would go out and detain suspected terrorists or insurgents, they would take the person and all of their papers, electronic devices, computers, all that type of stuff. They would bring them back to be reviewed and interrogated. So while the military was interrogating the suspect, my job would be to go through all of their electronic media and pull off whatever information was available.

03:23:36 **Q.** What was your first job in information technology --

03:23:40 **A.** My first --

03:23:41 **Q.** -- after you graduated?

03:23:42 **A.** My first job in information technology, I was a business analyst at Mutual of Omaha. And I worked up

03:23:50 through several jobs at Mutual of Omaha, from a business
03:23:54 analyst to a computer programmer, and then ultimately I was
03:23:57 a security analyst at Mutual of Omaha.

03:24:01 **Q.** Did you earn a bachelor's degree?

03:24:06 **A.** I did.

03:24:07 **Q.** From which institution did you earn that degree?

03:24:10 **A.** The University of Nebraska at Omaha.

03:24:12 **Q.** When did you earn the degree?

03:24:13 **A.** In 2003.

03:24:14 **Q.** What was the subject?

03:24:15 **A.** Management information systems.

03:24:18 **Q.** What is information systems?

03:24:21 **A.** Information systems is a, I guess a generic term for
03:24:25 computers.

03:24:26 **Q.** After earning your bachelor's degree, did you go on to
03:24:30 earn a master's degree?

03:24:31 **A.** I did.

03:24:32 **Q.** Where did you earn this degree?

03:24:34 **A.** Also from the University of Nebraska at Omaha.

03:24:37 **Q.** And what was the subject of your degree?

03:24:39 **A.** Management information systems.

03:24:44 **Q.** And when did you earn it?

03:24:45 **A.** In 2005.

03:24:48 **Q.** In addition to your education and work experience, have
03:24:55 you had the occasion to earn professional certifications?

03:25:00 **A.** I have.
03:25:00 **Q.** Could you explain to the jury some of the certifications
03:25:03 that you've earned and held?
03:25:05 **A.** Yes. So probably the biggest certification I've held
03:25:09 was I held a CISP, which is a very broad industry standard
03:25:15 certification for information security. And I've also held
03:25:19 multiple more specific certifications, several related to
03:25:24 computer forensics, one related to reverse engineering
03:25:29 malware, one related to computer networking devices, and,
03:25:34 you know, several other more generic ones.
03:25:39 **Q.** Through your education, your work experience with the FBI
03:25:44 and also prior to the FBI, have you become familiar with the
03:25:49 term "digital media" as it pertains to cyber investigations?
03:25:55 **A.** Yes, I am.
03:25:56 **Q.** Will you please explain to the jury what "digital media"
03:25:59 means and give some common examples?
03:26:01 **A.** Okay. So digital media is going to be anything that
03:26:05 can store data in a binary format or in a data format used
03:26:10 by computers. And that could include a computer, your cell
03:26:14 phone, the MMC card or the multimedia card you put into your
03:26:19 camera, a CD. It could be a, you know, electronic music
03:26:23 device. All of those would be considered digital media.
03:26:27 **Q.** Are you familiar with the term "forensic examination" as
03:26:31 it pertains to digital media?
03:26:33 **A.** I am.

03:26:33 **Q.** Will you please provide a basic definition of what this
03:26:38 means, "forensic examination"?
03:26:40 **A.** Yes. So for -- a forensic examination of digital media
03:26:44 is analyzing a piece of digital media -- so it could be a
03:26:49 computer, cell phone, anything -- in a manner which can be
03:26:52 replicated and verified by another person.
03:26:57 **Q.** Including your work in private industry, including your
03:27:02 time in Iraq and your time with the FBI, approximately how
03:27:09 many forensic examinations have you conducted?
03:27:12 **A.** I've performed over 100 examinations of digital media.
03:27:18 **Q.** And approximately how many hours of training have you
03:27:20 received in this field?
03:27:22 **A.** In the field specific of digital media examinations
03:27:26 or --
03:27:27 **Q.** Yeah.
03:27:29 **A.** I would say over a hundred hours of training.
03:27:33 **Q.** Will you please explain to the jury the basic steps in
03:27:38 conducting a forensic examination of digital media?
03:27:41 **A.** Okay. So the first basic step that's going to be
03:27:46 conducted when you are analyzing digital media is you are
03:27:49 going to make a copy of the original media. We call that a
03:27:52 forensic image. And the reason in which you do that is,
03:27:57 again, as I stated, computer forensics is conducting an
03:28:00 analysis in a way that's repeatable and able to be verified.
03:28:05 So when I take a forensic copy, I'm going to try to

03:28:08 work off of something that's not the original media in
03:28:11 case -- so that we limit or minimize the changes that occur
03:28:16 to the original evidence. And then we run a set of
03:28:20 standardized tools that will extract evidence from the
03:28:23 specific media type for the investigation that is being
03:28:26 conducted.

03:28:28 **Q.** And what types of files are you looking for during a
03:28:31 forensic examination of a hard drive in a computer intrusion
03:28:35 case?

03:28:36 **A.** So in a computer intrusion case we would generally be
03:28:39 looking for two general types of files. One is malicious
03:28:45 tools, so that could be malware or any additional file used
03:28:50 by the computer intruders. And then we are also looking for
03:28:54 files which contain information about how the malware was
03:28:59 executed on the system.

03:29:02 **Q.** So I think to back up and define computer intrusion -- I
03:29:06 should have done that earlier. What is a computer intrusion?

03:29:08 **A.** A computer intrusion is when somebody accesses a
03:29:14 computer without authorization or exceeds their
03:29:16 authorization.

03:29:17 **Q.** And I heard the word "malware."

03:29:24 **A.** Um-hmm.

03:29:24 **Q.** What is malware?

03:29:26 **A.** Malware is any code that is placed on a computer that
03:29:29 does something that the user doesn't want their computer to

03:29:32 do. So there's a lot of different types of malware.
03:29:36 **Q.** Are there common names that people use to refer to
03:29:40 malware?
03:29:41 **A.** Yes.
03:29:42 **Q.** What are some of those common names?
03:29:44 **A.** So a common term would be a computer virus, would be
03:29:49 what most people think about when they think of malware.
03:29:51 **Q.** Now, is there just one thing called malware, or are there
03:30:00 many types of malware?
03:30:02 **A.** There are many types of malware.
03:30:07 **Q.** Are you familiar with the term "remote access trojan"?
03:30:12 **A.** I am.
03:30:13 **Q.** Is that also referred to as a RAT?
03:30:17 **A.** It can be.
03:30:22 **Q.** Will you please explain to the jury what a remote access
03:30:26 trojan is?
03:30:27 **A.** A remote access trojan is a program on a computer that
03:30:31 provides remote access to the computer to a user that the
03:30:35 owner of the computer would prefer not to have access.
03:30:39 There are legitimate remote access tools, which especially
03:30:43 in current times with remote work you see commonly. But
03:30:47 what sets a RAT, or a remote access trojan, apart is that
03:30:51 the user or owner of the computer does not intend it to be
03:30:58 there.
03:30:58 **Q.** In general, how does a RAT or how does a remote access

03:31:03 trojan work?
03:31:04 **A.** There's two general ways a remote access trojan can
03:31:09 work. The first way is it can be installed on a computer
03:31:13 and it can open up the computer to access remotely on an
03:31:18 inbound connection from another location. So think of that
03:31:22 as it opens up the door. As long as somebody can see that
03:31:25 the door is open, they can walk in.
03:31:27 The other manner in which a remote access trojan can
03:31:31 operate is it can get installed on the computer and it can
03:31:33 initiate a connection outbound to some place on the Internet
03:31:38 to let the remote user or the remote intruder know that it's
03:31:44 there to be used.
03:31:45 **Q.** Is there a name for that process of the program reaching
03:31:52 out to a remote user?
03:31:53 **A.** Yes. We generally call that a beacon.
03:32:00 **Q.** Now, is there only one remote access trojan or are there
03:32:05 multiple versions of remote access trojan?
03:32:09 **A.** There are many versions of remote access trojans.
03:32:13 **Q.** Are you familiar with the term "Sakula"?
03:32:16 **A.** I am.
03:32:16 **Q.** What is Sakula?
03:32:19 **A.** Sakula is a specific type of remote access trojan.
03:32:25 **Q.** And just for the court reporter, it's S-A-K-U-L-A.
03:32:33 Will you explain to the jury how Sakula works?
03:32:38 **A.** Yeah. Sakula is a fairly basic remote access trojan.

03:32:42 So when it gets installed on a user's computer, it will
03:32:46 reach out to somewhere on the Internet with a beacon, and it
03:32:49 has a very specific beacon format. So there is a protocol
03:32:53 it uses to communicate with its controller on the Internet.
03:32:57 And what it allows the remote user to do is it can upload
03:33:01 files, download files, and run arbitrary commands on the
03:33:04 computer. It also can be told to uninstall itself.

03:33:10 **Q.** Does Sakula -- what, if any, remote access or control
03:33:16 does Sakula give somebody of a computer on which it is
03:33:21 installed?

03:33:22 **A.** So like I said before, they can run whatever commands
03:33:26 they want to at the command line of the system. They also
03:33:29 can upload and download files.

03:33:34 **Q.** How do you distinguish Sakula from another remote access
03:33:39 trojan?

03:33:40 **A.** We generally distinguish remote access trojans based on
03:33:48 two general things. One is the control that's present on
03:33:51 the disk; and the other thing, which is more pertinent to
03:33:54 this case, is the communication format that it uses when it
03:33:58 beacons.

03:34:00 **Q.** What does that mean in general terms, the communication
03:34:06 format it uses to beacon?

03:34:08 **A.** We call that a communication protocol. So what a
03:34:11 communication protocol is, is the way two things
03:34:14 communicate. In this case it's on the Internet, but it can

03:34:16 be in your normal, everyday life.
03:34:18 So a good example of a communication protocol would be
03:34:21 if you want to make a phone call to somebody else in the
03:34:24 U.S., you pick up the phone, you dial the number that you
03:34:27 want to call. You start to hear it ring. So that's the
03:34:30 first part of the protocol. The other person hears it ring
03:34:34 on their end, and they pick up the phone. When they pick up
03:34:36 the phone -- in my case I say, "Hello. This is Adam." Then
03:34:42 you know that you have established a communication that is
03:34:44 an English phone call.
03:34:47 **Q.** Are you familiar with the term "plugX."
03:34:53 **A.** I am.
03:34:54 **Q.** What is plugX?
03:34:55 **A.** PlugX is a variant of a remote access trojan.
03:34:59 **Q.** In general terms, how does plugX work?
03:35:03 **A.** PlugX works very similar to Sakula. It gets installed
03:35:08 on a computer, and it will initiate a beacon outbound to a
03:35:12 predefined location on the Internet.
03:35:16 **Q.** Does plugX have a different protocol than Sakula?
03:35:20 **A.** It does.
03:35:21 **Q.** Is the ultimate affect of providing remote access
03:35:25 similar, though?
03:35:25 **A.** It is similar.
03:35:27 **Q.** Just one more term I'd like to loop back to. Are you
03:35:32 familiar with the phrase "executable file"?

03:35:36 **A.** I am.

03:35:37 **Q.** Could you provide a basic definition of what this term
03:35:42 means and provide a couple examples of what are executable
03:35:47 files?

03:35:47 **A.** An executable file is a program that can be run on a
03:35:50 computer. So a good example of an executable file is if you
03:35:55 go to your computer or your phone or whatever you use to
03:35:57 browse the Internet and you click on the icon that opens up
03:36:00 a web browser, what the computer in the background is doing
03:36:03 is opening up an executable file that causes the browser to
03:36:08 be displayed to you, which then allows you to be connected
03:36:12 to the Internet.

03:36:12 **Q.** I'd like to direct your attention now to October of 2019.
03:36:18 Did there come a time that you conducted a forensic
03:36:20 examination of a hard drive?

03:36:23 **A.** Yes, I did.

03:36:24 **Q.** Who provided you with the hard drive?

03:36:27 **A.** The hard drive was provided by DGSI.

03:36:32 **Q.** What is DGSI?

03:36:34 **A.** DGSI is roughly equivalent to the domestic
03:36:40 investigation and intelligence arm of the French government
03:36:44 as it relates to cyber matters.

03:36:47 **Q.** Does it have a law enforcement component to it?

03:36:49 **A.** Yes, it does.

03:36:51 **Q.** And does the FBI and DGSI have a law enforcement

03:36:55 relationship?

03:36:56 **A.** We do.

03:36:57 **Q.** And as a result of this relationship, did they share this
03:37:01 computer with you?

03:37:02 **A.** Yes.

03:37:03 **Q.** Did you then conduct a forensic examination of the
03:37:08 computer -- or of the hard drive? Excuse me.

03:37:11 **A.** Yes, I did.

03:37:12 **Q.** As part of that examination, were you able to determine
03:37:19 what computer system and network the hard drive belonged to?

03:37:23 **A.** Yes.

03:37:24 **Q.** And what company, if any, did the hard drive belong to?

03:37:30 **A.** So the company was registered -- sorry. The hard drive
03:37:34 was registered to Snecma.

03:37:37 **Q.** And what is Snecma?

03:37:40 **A.** Snecma is a subsidiary of Safran Group.

03:37:44 **Q.** And where is Safran located?

03:37:46 **A.** Safran is headquartered in France.

03:37:49 **Q.** And as part of your examination of the hard drive, were
03:37:53 you able to identify a user profile?

03:37:57 **A.** Yes, I was.

03:37:58 **Q.** Were you able to view emails and other documents?

03:38:04 **A.** Yes, I was.

03:38:05 **Q.** Were you able to identify a particular user of that hard
03:38:11 drive as a result of your analysis?

03:38:14 **A.** Yes.

03:38:14 **Q.** Was that person Frederic Hascoet?

03:38:19 **A.** It was.

03:38:20 **Q.** Will you please provide the jury with an overview of how
03:38:26 you conducted the forensic examination of this hard drive?

03:38:30 **A.** Yes. So we first took a forensic image of the hard
03:38:35 drive, and then I conducted analysis against the forensic
03:38:38 image. The first step that I did is I created a timeline of
03:38:43 activities that were on the system, and then I reviewed the
03:38:47 timeline to see if there was any indication of a computer
03:38:50 intrusion.

03:38:51 **Q.** As a result of your analysis, what, if any, malware did
03:39:00 you find?

03:39:00 **A.** On the hard drive, I found one variant of Sakula
03:39:07 malware and two variants of plugX.

03:39:11 **Q.** Were you able to determine when these malware programs
03:39:15 were installed on the hard drive?

03:39:16 **A.** Yes.

03:39:17 **Q.** I'll come -- I'll come back to that.
03:39:22 I'd like to start with a discussion of Sakula. Was there
03:39:29 just one file associated with Sakula or were there multiple
03:39:35 files associated with this program?

03:39:37 **A.** For Sakula, there was two files still on disk that were
03:39:41 related to Sakula.

03:39:44 **Q.** Were you able to determine what Sakula was set up to do?

03:39:48 **A.** Yes, I was.
03:39:50 **Q.** Will you please explain that to the jury?
03:39:53 **A.** The Sakula variant that was located on the hard drive I
03:39:57 analyzed was set up to initiate beacons to two domains on
03:40:04 the Internet.
03:40:04 **Q.** What is a domain?
03:40:08 **A.** A domain is a shortened version of domain name. So a
03:40:12 domain name is how normal people access locations on the
03:40:17 Internet. So computers communicate via IP addresses. So
03:40:22 think of an IP address of a computer as similar to your
03:40:26 telephone number.
03:40:26 A domain name would be equivalent to setting up a
03:40:29 contact in your phone to link a phone number to a name that
03:40:33 you remember. So like if I want to go to www.fbi.gov,
03:40:39 that's what I type in my web browser. But on the back end,
03:40:43 the domain name system is doing the correlation between
03:40:50 www.fbi.gov and an IP address that is assigned to that
03:40:56 domain.
03:40:57 **Q.** Quickly, for the IP address, does the "IP" stand for
03:41:02 Internet protocol?
03:41:03 **A.** It does.
03:41:04 **Q.** Is it a series of numbers and periods?
03:41:08 **A.** Essentially, yes.
03:41:09 **Q.** Okay.
03:41:09 THE COURT: Have we reached an opportunity where we

03:41:10 could break?

03:41:12 MR. McKENZIE: Of course, Your Honor.

03:41:13 THE COURT: Very well. We're going to take a
03:41:16 20-minute break and going to come back at 4. And it would
03:41:19 appear you are going to survive. During the break, please
03:41:23 take a break. Don't discuss the case among yourselves or with
03:41:25 anyone else. No independent research. Continue to keep an
03:41:29 open mind.
03:41:31 Out of respect for you, we will rise as you leave.

03:41:34 THE COURTROOM DEPUTY: All rise for the jury.

03:41:36 (Jury out at 3:41 p.m.)

03:42:06 THE COURT: The jury's left the room. The door is
03:42:19 closed.
03:42:20 We're going to recess till 4. It's almost 20 minutes.
03:42:24 And then when we come back at 4, what's the likelihood that
03:42:28 the government will finish direct?

03:42:30 MR. McKENZIE: Zero percent, Your Honor.

03:42:32 THE COURT: Zero percent.

03:42:34 MR. McKENZIE: Zero percent.

03:42:35 THE COURT: So he is not going home to San Diego
03:42:40 tonight.

03:42:44 MR. McKENZIE: Not tonight, Your Honor.

03:42:46 THE COURT: We are in recess until 4. Hoping to
03:42:48 break at 4:30.

03:42:48 THE COURTROOM DEPUTY: All rise. We are in recess

03:42:50 until 4 p.m.

03:42:53 (Recess from 3:43 p.m. until 3:59 p.m.)

03:59:58 THE COURT: Back on the record, about to get the
04:00:05 jury.

04:00:05 Mr. McKenzie, have the odds changed?

04:00:08 MR. McKENZIE: You know, I took another look at my
04:00:11 outline, and I bump up to maybe five percent. I'm feeling a
04:00:15 little more bullish.

04:00:16 THE COURT: Let the record reflect that.

04:00:19 Are we ready for the jury from the government's
04:00:21 perspective?

04:00:22 MR. McKENZIE: Yes, Your Honor.

04:00:22 THE COURT: And the defense?

04:00:24 MS. TAYLOR: Yes, Your Honor.

04:00:25 THE COURT: Very well. Let's call for the jury.

04:01:17 We need to remember we have an interpreter at the end of
04:01:20 a long day, so if we can all try and talk slowly, that will
04:01:25 accommodate her.

04:01:32 THE COURTROOM DEPUTY: All rise for the jury.

04:01:34 (Jury in at 4:01 p.m.)

04:02:05 THE COURT: You may all be seated. Thank you.

04:02:10 15 jurors have returned from a break. We will continue
04:02:15 hearing testimony from this witness, who remains under oath.

04:02:19 The prosecutor may continue.

04:02:19 BY MR. McKENZIE:

04:02:24 **Q.** Before the break, we were defining what a domain name is.
04:02:33 And prior to that, you testified about Sakula beaconing to a
04:02:41 domain name.
04:02:43 How many domains, if any, did the Sakula malware beacon
04:02:50 to?
04:02:50 **A.** It was configured to beacon to two domain names.
04:02:53 **Q.** And were there particular domain names that the malware
04:02:58 beaconed to?
04:02:59 **A.** Yes, there were.
04:03:01 **Q.** Do you remember those domain names?
04:03:04 **A.** I do.
04:03:04 **Q.** What was the first domain it beaconed to?
04:03:10 **A.** The first domain was oa.ameteksen.com.
04:03:19 **Q.** Are you familiar with a company called Ametek Sensors?
04:03:25 **A.** I am.
04:03:26 **Q.** What is Ametek Sensors?
04:03:29 **A.** Ametek Sensors is a subsidiary of a larger company
04:03:35 named Ametek, which is a part supplier for Snecma.
04:03:42 **Q.** And by part supplier, is that like airline parts?
04:03:45 **A.** Yes.
04:03:46 **Q.** Does Ametek Sensors have a website?
04:03:53 **A.** Yes, they do.
04:03:54 **Q.** Have you visited that website?
04:03:56 **A.** I did at the time.
04:04:00 **Q.** Are you familiar with the term "doppelganger domain"?

04:04:09 **A.** I am.
04:04:10 **Q.** Would you please explain to the jury what a doppelganger
04:04:14 domain is?
04:04:15 **A.** Doppelganger domain is a domain name that's intended to
04:04:20 look similar to a legitimate company's domain but it's not
04:04:23 owned by the legitimate company.
04:04:25 **Q.** And how are doppelganger domains used in computer
04:04:32 intrusions and in cyber investigations?
04:04:33 **A.** There are several ways that doppelganger domains can be
04:04:38 used in computer intrusion activity. One good example is if
04:04:42 I wanted to click on something that has malicious -- some
04:04:46 kind of malicious attachment. If I send you a domain name
04:04:50 that is maybe one letter off of something you're likely to
04:04:55 go to, it's going to be more likely to entice you to click
04:04:58 on that link and download the malware.
04:05:01 Another way, which is more pertinent to this instance,
04:05:04 is when a company has any kind of computer on their internal
04:05:12 network trying to reach out to something on the Internet,
04:05:15 they monitor those systems to make sure they are --
04:05:20 generally their users are going to places they should be.
04:05:23 And so if you create a doppelganger domain and put it in
04:05:27 malware, when it beacons out to the Internet it looks like
04:05:30 more legitimate traffic.
04:05:32 **Q.** Did you investigate or look into oa.ameteksen.com?
04:05:47 **A.** Yes, I did.

04:05:47 **Q.** Is that a web domain name owned by Ametek Sensors?
04:05:49 **A.** It is not.
04:05:50 **Q.** Now, you mentioned that the Sakula malware beaconed to a
04:06:04 second domain. Will you please share that second domain with
04:06:07 the jury?
04:06:08 **A.** The second domain that it was configured to beacon to
04:06:11 was secure.safran-group.com.
04:06:18 **Q.** Are you familiar with Safran Group, the company?
04:06:22 **A.** I am.
04:06:23 **Q.** Did you visit secure.safran-group.com?
04:06:31 **A.** I did not directly visit that domain.
04:06:33 **Q.** Are you aware if safran-group.com is a legitimate domain
04:06:38 owned by Safran, the company?
04:06:40 **A.** It is owned by Safran, the company.
04:06:44 **Q.** Backing up to your forensic analysis. Were you able to
04:06:53 determine if Sakula actually did beacon to these domains?
04:06:59 **A.** I was able to determine that.
04:07:00 **Q.** And how do you know?
04:07:01 **A.** There was evidence located on the hard drive of
04:07:07 outbound connections to both of those domains in the format
04:07:09 of a Sakula beacon.
04:07:11 **Q.** Now, you mentioned earlier that there were more than one
04:07:20 file -- that there was more than one file associated with this
04:07:24 Sakula malware. Did any of those files have visible
04:07:34 interfaces that you could interact with and see on the screen

04:07:37 of the computer?
04:07:37 **A.** Yes, one of them did.
04:07:41 **Q.** In which language was that program?
04:07:43 **A.** It was in the Chinese language.
04:07:46 **Q.** Were you able to determine when the Sakula malware was
04:07:55 installed on the hard drive?
04:07:58 **A.** I was.
04:07:59 **Q.** And what date was the malware installed on the hard
04:08:05 drive?
04:08:05 **A.** January 25th of 2014.
04:08:09 **Q.** How do you know it was January 25th of 2014?
04:08:14 **A.** Because evidence associated with the file, like the
04:08:18 created date indicated it was that date.
04:08:22 **Q.** What, if anything significant, happened with the hard
04:08:27 drive prior to Sakula being installed on the computer? What,
04:08:34 if anything, from the log?
04:08:36 **A.** There was several things that happened. A USB device
04:08:40 was inserted into the computer immediately before the
04:08:48 installation.
04:08:48 **Q.** What is a USB drive?
04:08:51 **A.** A USB device is a piece of removable media that is
04:08:55 generally used by people to store files to transfer between
04:08:59 computers.
04:08:59 **Q.** How do you know that a USB drive was installed into the
04:09:02 computer before the Sakula malware was installed?

04:09:09 **A.** So when a user takes actions on a computer, the
04:09:13 operating system of that computer records information about
04:09:15 the actions that were taken. Generally, these are being
04:09:20 recorded to improve the user experience on the computer.
04:09:24 And so when you insert a USB device into a computer, the
04:09:28 computer records information about that USB device. So if
04:09:32 you plug the same one in again in the future, your user
04:09:36 experience is going to be as close to as possible as the
04:09:38 first time you inserted it.
04:09:41 **Q.** On what date was the USB drive installed into the hard
04:09:45 drive?
04:09:46 **A.** It was inserted into the computer on --
04:09:50 **Q.** Into the computer. I'm sorry.
04:09:55 **A.** -- on January the 25th, 2014.
04:09:58 **Q.** I'd like to take a step back from your forensic
04:10:01 examination for a moment.
04:10:07 As part of your investigation, did you review text
04:10:09 messages sent and received by the defendant?
04:10:13 **A.** I did.
04:10:14 MR. McKENZIE: Before we get to those, Your Honor, I
04:10:16 ask that we publish to the jury Government's Exhibit 21b,
04:10:22 which is already in evidence, and I ask that we turn to page
04:10:26 1.
04:10:27 THE COURT: Very well.
04:10:31 BY MR. McKENZIE:

04:10:32 **Q.** Directing your attention to page 1, could you please read
04:10:34 the name listed in the top left corner?
04:10:38 **A.** Xu Yanjun.
04:10:42 **Q.** Moving to the middle of the page, can you read what is
04:10:45 written under "Current Post"?
04:10:49 **A.** "Deputy division director at Sixth Bureau of Jiangsu
04:10:54 Province Ministry of State Security."
04:10:56 **Q.** I'd like to direct your attention now to page 2. And
04:11:02 specifically to the job posting from August 2010 to November
04:11:10 2014. Could you please read that job posting?
04:11:15 **A.** "Section chief at Second Section of Fourth Bureau of
04:11:22 Jiangsu Ministry of State Security, the agency renamed to
04:11:26 the Sixth Bureau in December, 2013."
04:11:28 THE COURT: Sir, you are doing great. Can you keep
04:11:30 your voice up, please. A couple old men in the back row
04:11:33 having trouble hearing you.
04:11:36 THE WITNESS: Do you want me to read it again?
04:11:39 THE COURT: No.
04:11:40 BY MR. McKENZIE:
04:11:40 **Q.** No.
04:11:42 MR. McKENZIE: Your Honor, may we now publish what
04:11:44 is in evidence as Government's Exhibit 110, and direct the
04:11:50 witness's attention to page 1?
04:11:55 THE COURT: Yes.
04:11:59 BY MR. McKENZIE:

04:12:02 **Q.** Looking at the key at the very, very top, in what color
04:12:06 are the messages sent by Xu Yanjun?
04:12:10 **A.** Blue.
04:12:13 **Q.** Will you please read the first message sent on November
04:12:20 19, 2013?
04:12:23 **A.** Xu Yanjun contacted Tian Xi. He said, "On what date
04:12:31 does the Frenchman arrive? Is it possible to make
04:12:34 arrangements for him to meet with Teacher Wu Tieying and I
04:12:40 in Suzhou? Under the name of Nanjing University of
04:12:47 Aeronautics and Astronautics in the evening."
04:12:48 **Q.** In what country is Safran located?
04:12:50 **A.** They are located in France.
04:12:52 **Q.** Who sent this message that you just read?
04:12:54 **A.** Xu Yanjun.
04:12:58 **Q.** And who received the message?
04:12:59 **A.** Tian Xi.
04:13:02 MR. McKENZIE: Your Honor, I ask that we now show
04:13:04 the witness what is in evidence as Government's Exhibit 111.
04:13:09 And I ask that we direct the -- or excuse me -- publish to the
04:13:15 jury 111 and direct the witness's attention to page 6.
04:13:21 THE COURT: Yes.
04:13:28 BY MR. McKENZIE:
04:13:28 **Q.** I am showing you what is in evidence as Government's 111.
04:13:31 Are these business records from Safran?
04:13:33 **A.** Yes, it is.

04:13:34 **Q.** Directing your attention to the -- the top of the page,
04:13:43 who is the sender of this letter?
04:13:45 **A.** Safran Aircraft Engines Suzhou Company, Limited.
04:13:51 **Q.** Turning your attention to the first paragraph of the
04:13:56 column on the right. Who is the recipient of this letter?
04:14:00 **A.** Tian Xi.
04:14:04 **Q.** About midway through there is a title. Will you please
04:14:08 read the title of this letter?
04:14:10 **A.** "Position of Manufacturing Engineer."
04:14:13 **Q.** Under "Re:" -- do you see where it says "Re: Termination
04:14:18 Letter"?
04:14:18 **A.** Oh, yes.
04:14:19 **Q.** And then directing your attention to the first full
04:14:22 paragraph, does it list Tian Xi's position as manufacturing
04:14:30 engineer?
04:14:30 **A.** It does.
04:14:31 **Q.** We'll return to this exhibit later. I would like to
04:14:41 please go back to Government's 110, page 1.
04:14:47 I will read the responses from Tian Xi, and you please
04:14:55 read the messages for Xu Yanjun.
04:14:58 Tian responded, "Next Monday. I'll be here with another
04:15:03 Frenchman that frequently comes to Suzhou. I think they will
04:15:08 be together all the time. It's not good to talk to both of
04:15:10 them. I will [mention] it to him."
04:15:16 "Mention it to him and see what reaction he has."

04:15:21 **A.** Xu Yanjun then replies, "Good, thanks."

04:15:25 **Q.** Moving to November 25, 2013, will you again read the 04:15:32 messages from Xu Yanjun, and I will read the messages from 04:15:39 Tian Xi.

04:15:40 **A.** "Do you have any knowledge of the company Firth Rixon 04:15:45 Company?"

04:15:45 **Q.** "The Suzhou Company isn't far from us but I've no 04:15:48 knowledge of it."

04:15:50 **A.** "Are those two Frenchmen arriving today? Are they 04:15:53 going to Shanghai together on the weekend?"

04:15:57 **Q.** "Yes."

04:15:57 **A.** "What's the other Frenchman's name? What position does 04:16:00 he hold? Is it his first time here? Will come often in the 04:16:05 future? Are you familiar with him?"

04:16:08 **Q.** "Both come often. One has been here ten times or so this 04:16:11 year. The other's office is next door. First time coming 04:16:15 over."

04:16:17 **A.** "Do you have their business cards? If not, can you get 04:16:20 them?"

04:16:21 **Q.** "I have one. Will ask the other one."

04:16:24 **A.** "Okay. Please help me to get the information. I'm 04:16:28 sending what I need to your email. Thanks."

04:16:31 **Q.** "Got it."

04:16:32 **A.** "Email sent. Please check."

04:16:33 **Q.** "Okay."

04:16:36 Will you please read the message from November 26, 2013?
04:16:40 **A.** "When is it convenient for you to talk on the phone?"
04:16:47 **Q.** Will you please read the last message on this page from
04:16:52 November 27, 2013?
04:16:55 **A.** "I'll bring the horse to you tonight. Can you take the
04:16:59 Frenchman out for dinner tonight? I'll pretend I bump into
04:17:04 you at the restaurant to say hello. This way we don't need
04:17:08 to meet in Shanghai."
04:17:10 **Q.** Who sent that message?
04:17:12 **A.** Xu Yanjun.
04:17:15 **Q.** To whom did he send it?
04:17:17 **A.** Tian Xi.
04:17:19 **Q.** What does the phrase "horse" mean in cyber
04:17:21 investigations?
04:17:22 **A.** Remote access trojan.
04:17:24 **Q.** Where does the horse -- how does trojan derive -- let me
04:17:30 rephrase. How do you get "horse" from the phrase "trojan"?
04:17:34 **A.** Yes. So the name "remote access trojan" in computer
04:17:38 security is taken from the old Greek mythology of the trojan
04:17:43 horse. So in that story in Greek mythology the Greeks built
04:17:47 a trojan horse. They enticed the trojans to bring it inside
04:17:50 their city, and then it allowed -- you know, some soldiers
04:17:53 got out and opened the gates to allow the Greek Army in.
04:17:57 And so that's similar to a piece of malware being
04:18:01 installed on your computer and then allowing your remote

04:18:05 user to access it, similar to how it was used Greek mythology.

04:18:08 **Q.** Is a remote access trojan a type of trojan horse?

04:18:11 **A.** It is.

04:18:12 **Q.** Is Sakula a type of trojan horse?

04:18:14 **A.** It is.

04:18:14 **Q.** And remind me, where is Safran located?

04:18:20 **A.** It's headquartered in France.

04:18:23 MR. McKENZIE: Could we please see page 2 of Exhibit 110.

04:18:27 BY MR. McKENZIE:

04:18:31 **Q.** I'd like to continue reading the messages from November 27th. I will read Tian Xi.

04:18:39 He responded, "I will find out if they have other arrangements."

04:18:42 **A.** "Good. Is tonight on?"

04:18:44 **Q.** "No."

04:18:47 **A.** "I'm on the train. Be in Suzhou around five."

04:18:51 "Best to have dinner arrangement for tonight. If not, I'll stay at the hotel where they stay and then you can say we'll have breakfast with them tomorrow morning and can go to work together. This way I can also meet them."

04:19:07 "Most important is to meet them face to face."

04:19:11 **Q.** "Got it. They'll have a telephone conference call this afternoon with France. I am discussing with them the matter

04:19:18 of having dinner tonight."
04:19:25 I'd like to move on to the next set of messages.
04:19:33 "It's possible they don't get off work until rather
04:19:37 late."
04:19:37 **A.** "Okay."
04:19:38 "It's tough."
04:19:40 "If you're successful in arranging a meal, where would
04:19:43 it be? I'll soon be in Suzhou."
04:19:47 "I can wait for you there first."
04:19:49 "I'm in a taxi, first heading to Yinxiang City."
04:19:55 **Q.** "Let's meet in Yinxizng City. They're having a telephone
04:19:58 conference meeting and will be late."
04:20:01 **A.** "Good."
04:20:02 **Q.** "They are going straight to eat at the hotel today."
04:20:06 **A.** "I am here."
04:20:07 "I'm on the fourth floor, Dayu. Waiting for you at the
04:20:13 booth seat in the back."
04:20:15 **Q.** "Haven't left work yet. Wait an hour for me."
04:20:18 **A.** "No worry, this is a buffet. I can wait."
04:20:22 "Which hotel are they staying at?"
04:20:24 **Q.** "Crowne Plaza."
04:20:27 **A.** "I've arrived."
04:20:31 **Q.** Let's continue to read the messages from November 29,
04:20:36 2013.
04:20:39 **A.** "No chance these two days?"

04:20:41 **Q.** "Not yet. I'll pay attention."

04:20:50 **A.** "Good."

04:20:51 MR. McKENZIE: Can we turn to the next page, please.

04:20:51 BY MR. McKENZIE:

04:20:54 **Q.** Will you please read the first message from December 6, 04:20:58 2013?

04:20:58 **A.** "Horse hasn't been planted."

04:21:01 **Q.** Who sent that message?

04:21:02 **A.** Xu Yanjun.

04:21:04 **Q.** To whom did he send it?

04:21:05 **A.** Tian Xi.

04:21:09 **Q.** In the context of cyber investigations, what does it mean 04:21:12 to plant a horse?

04:21:13 **A.** To install a remote access trojan.

04:21:16 **Q.** Let's continue reading the messages.

04:21:20 "Not yet. I'll replay your email this weekend."

04:21:24 **A.** "Good."

04:21:28 **Q.** And let's continue on to December 9, 2013.

04:21:34 **A.** "Have you sent the email to me?"

04:21:36 **Q.** "Will send tonight, sorry about that."

04:21:39 **A.** "It's nothing. Ho, ho."

04:21:45 **Q.** And we'll continue on to the 26th of December.

04:21:51 **A.** "That old man came over this time but still can't find 04:21:54 an opportunity?"

04:21:56 **Q.** "No. Will notify you when it's planted."

04:22:03 Again, what does "planted" mean in this context?

04:22:06 **A.** To install a remote access trojan.

04:22:11 **Q.** Directing your attention to the first message of January
04:22:16 16, 2014. Will you please read just the first message?

04:22:23 **A.** "Little Gu, will you be in Suzhou tomorrow?"

04:22:29 **Q.** Who sent that message?

04:22:30 **A.** Xu Yanjun.

04:22:33 **Q.** And who received the message?

04:22:34 **A.** Gu Gen.

04:22:38 MR. McKENZIE: Your Honor, at this time I ask
04:22:40 permission to publish to the jury what is in evidence as
04:22:43 Government's 111 and show the jury page 1.

04:22:49 THE COURT: Yes, it's in evidence. I thought we
04:22:52 were just looking at that.

04:22:54 MR. McKENZIE: Yes.

04:22:54 THE COURT: Okay. Page 1.

04:22:54 BY MR. McKENZIE:

04:22:59 **Q.** Directing your attention to the top left of the page,
04:23:02 what is listed under "Name"?

04:23:05 **A.** Gu Gen.

04:23:07 **Q.** Near the bottom of the screen that's being displayed
04:23:10 right now, will you please read what it is in the box next to
04:23:16 "Position"?

04:23:16 **A.** "Senior IT infrastructure manager and information
04:23:20 security officer."

04:23:22 **Q.** Directing your attention to the bottom of the page, which
04:23:26 will require a scroll down, will you please read who is listed
04:23:31 as the employer where we have that stamp?
04:23:34 **A.** It says, "Safran Beijing Enterprise Management Company
04:23:39 Limited, Suzhou Branch."
04:23:43 **Q.** All right.
04:23:45 MR. McKENZIE: Your Honor, I ask to return to
04:23:47 Government's 110, page 3, and publish that now to the jury.
04:23:51 THE COURT: Yes.
04:23:55 MR. McKENZIE: And could we scroll down now to the
04:23:58 messages on January 16th.
04:23:58 BY MR. McKENZIE:
04:24:02 **Q.** I will read the Gu Gen response.
04:24:07 "Yes."
04:24:08 **A.** "I may go to Suzhou tomorrow. Let's meet if you are
04:24:14 available."
04:24:15 **Q.** "Okay."
04:24:17 Can we please read the first set of messages on January
04:24:24 17, 2014? And we'll stop when we get to 11:07 a.m.
04:24:36 **A.** Okay.
04:24:36 "Let's meet in the evening at Yinxiangcheng."
04:24:39 "What time do you prefer?"
04:24:42 **Q.** Gu Gen replied, "I should be able to get there around 6."
04:24:47 **A.** "Okay."
04:24:48 "Little Gu, my schedule changed. I may arrive in

04:24:52 Suzhou late. Shall we meet at 8 instead? Still in 'Tea and Seat' in Yinxiangcheng. Let's just have a chat instead of dinner. What do you think?"

04:25:05 "Sorry about that."

04:25:07 **Q.** "8 o'clock is a little bit too late. What about we do a phone chat instead?"

04:25:12 **A.** "It won't take long. 30 minutes will do. I will arrive in Suzhou around 7. I can be there by 7:30 at the earliest."

04:25:21 **Q.** "Okay."

04:25:22 **A.** "I got on an earlier train. Will arrive at Yinxiangcheng in 30 minutes."

04:25:30 MR. McKENZIE: Can we please go to page 4.

04:25:30 BY MR. McKENZIE:

04:25:35 **Q.** "Okay. I'm on my way."

04:25:36 **A.** "I have arrived."

04:25:38 **Q.** "Will be there soon."

04:25:39 **A.** "No hurry."

04:25:41 **Q.** Let's -- let's stop right there.

04:25:44 I'm going to direct your attention to just the next message. Will you please read that message?

04:25:55 **A.** "I just met with Little Gu and he said Safran cautioned people were posing as company leadership sending out letters. Did you all do that?"

04:26:06 **Q.** Who sent that message?

04:26:08 **A.** Xu Yanjun.

04:26:10 **Q.** To whom did he send it?

04:26:12 **A.** Chai Meng.

04:26:16 MR. McKENZIE: Your Honor, I ask that we publish to
04:26:18 the jury what is in evidence as Government's 39b and direct
04:26:22 their attention to page 1.

04:26:25 THE COURT: Yes.

04:26:25 BY MR. McKENZIE:

04:26:29 **Q.** Directing your attention to the fourth message sent on
04:26:36 the right there. Is that the message that you just read?

04:26:39 **A.** That is what I just read.

04:26:42 **Q.** And is the recipient there on the left Chai Meng?

04:26:49 **A.** Yes, it is.

04:26:50 MR. McKENZIE: Your Honor, I'd like to return now to
04:26:52 the Government's Exhibit 110, where we left off.

04:26:57 THE COURT: Very well.

04:26:58 MR. McKENZIE: Page 4? Page 3. I apologize. With
04:27:02 the Chai Meng. No, page 4. On page 4.

04:27:02 BY MR. McKENZIE:

04:27:10 **Q.** And I will read Chai Meng's response.

04:27:13 "We pretended to be the webmaster sending out the letter
04:27:17 but not posing as leadership. It's unknown how many want to
04:27:20 engage Safran each day."

04:27:22 **A.** "How is it that you all didn't bother them by
04:27:25 cautioning? I just stated that it was you that had done

04:27:30 it."

04:27:30 **Q.** "Gu believed we did it?"

04:27:33 **A.** "No doubt."

04:27:34 **Q.** Are you familiar with the term "phishing," spelled
04:27:41 P-H-I-S-H-I-N-G, in the context of cyber intrusions?

04:27:46 **A.** I am.

04:27:47 **Q.** Will you explain to the jury what phishing is?

04:27:52 **A.** Phishing is when you send an email to somebody that
04:27:55 looks like an email that they would get from a person that
04:27:58 they would expect to get an email from, but what you do is
04:28:01 you embed some kind of either malicious link or you add a
04:28:05 malicious attachment that if they click on it or open the
04:28:08 attachment, it will compromise their computer and give you
04:28:11 access to it.

04:28:13 **Q.** What stands out to you about this exchange that we just
04:28:18 read?

04:28:19 **A.** What stands out to me most is that Gu had told them
04:28:26 that Safran had cautioned people, that people were posing as
04:28:31 the leadership to send out letters, which could also be
04:28:35 emails.

04:28:37 **Q.** I'd like to pause from reading these messages for a
04:28:41 moment and return to your analysis of the computer.
04:28:44 On which date was the Sakula malware you found installed
04:28:49 on the computer?

04:28:50 **A.** January 25th of 2014.

04:28:55 **Q.** On which date was the USB drive installed on the
04:28:58 computer?
04:28:59 **A.** It was inserted into the computer on January 25, 2014.
04:29:03 **Q.** Returning to the Government's Exhibit 110, I would like
04:29:08 to begin reading the messages from January 25, 2014. Is this
04:29:14 the same day that the malware was installed?
04:29:17 **A.** It is.
04:29:17 **Q.** Will you please read, even though it's in green, but will
04:29:21 you please read the first message from January 25, 2014?
04:29:26 **A.** "The horse is planted this morning."
04:29:29 **Q.** Will you please remind the jury what it means to plant a
04:29:32 horse?
04:29:32 **A.** To install a remote access trojan.
04:29:35 **Q.** Who sent that message?
04:29:36 **A.** Tian Xi.
04:29:39 **Q.** To whom did he send it?
04:29:43 **A.** Xu Yanjun.
04:29:43 **Q.** Will you please read just the defendant's response?
04:29:52 **A.** "Good."
04:29:54 **Q.** Now, the next message on the screen, who sent that
04:30:01 message?
04:30:02 **A.** Xu Yanjun.
04:30:03 **Q.** To whom did he send it.
04:30:05 **A.** Chai Meng.
04:30:07 **Q.** What did the defendant tell Chai Meng?

04:30:09 **A.** "I have reported the Suzhou incident to Zha, and I will
04:30:14 start my vacation today. Please direct any inquiries or
04:30:17 reports to Chen. Thanks."
04:30:19 **Q.** I will now read Chai Meng's response.
04:30:25 "Okay. A device with a Nanjing IP address is now online.
04:30:30 I'm taking a look at."
04:30:35 Will you please remind the jury what an IP address is?
04:30:41 **A.** An IP address is how a device that's on the Internet is
04:30:46 communicated with. So it's the address at which that device
04:30:50 is located.
04:30:51 **Q.** What does it mean to have a Nanjing IP address?
04:30:57 **A.** There are ways to geolocate, so to determine where a
04:31:01 physical computer is, based on the IP address. So in this
04:31:05 instance, they indicate that the IP address is geolocating
04:31:11 to Nanjing.
04:31:12 **Q.** In the context of remote access trojans in general and
04:31:17 Sakula in particular, what does it mean to be online?
04:31:21 **A.** To be online for remote access trojan means that the
04:31:26 beacon has been received by a controller that is controlled
04:31:29 by the IP intruders.
04:31:31 **Q.** Based on your review of the Sakula malware, does that
04:31:35 program allow a user to take a look at the computer?
04:31:38 **A.** Yes, it would allow them to access the computer.
04:31:44 **Q.** Will you please read the next message?
04:31:51 **A.** "I saw this person's device, but his IP shows Nanjing.

04:31:56 Is that person in Nanjing?"

04:31:58 **Q.** Who sent that message?

04:31:59 **A.** Xu Yanjun.

04:32:02 **Q.** To whom did he send it?

04:32:04 **A.** Tian Xi.

04:32:06 **Q.** And how did Tian Xi respond?

04:32:10 **A.** "No, he is in Suzhou."

04:32:14 **Q.** Directing your attention now to January 26, 2014,
04:32:20 messages, will you please read the first message that was
04:32:23 sent?

04:32:25 **A.** "Destroy the horse."

04:32:28 **Q.** Who sent that message?

04:32:29 **A.** Xu Yanjun.

04:32:32 **Q.** To whom did he send it?

04:32:34 **A.** Tian Xi.

04:32:35 **Q.** Did Tian Xi reply, "Acknowledged"?

04:32:39 **A.** He did.

04:32:41 THE COURT: We are past 4:30. Are we at a good
04:32:44 break point?

04:32:45 MR. McKENZIE: As good as any, Your Honor.
04:32:47 Actually, you know what? If I can ask two more
04:32:50 questions, we will be at an even better break point.

04:32:54 THE COURT: I'll count them. Go ahead.

04:32:54 BY MR. McKENZIE:

04:32:59 **Q.** Question 1: Based on your review, your forensic review

04:33:02 of the computer, was the Sakula malware altered on January 26,
04:33:10 2014?

04:33:11 **A.** It was not.

04:33:11 **Q.** In this context, what does "destroy the horse" mean?

04:33:18 **A.** In this context, it could mean to either remove the
04:33:20 malware from the compromised computer or to destroy the
04:33:25 device that the horse was originally located on.

04:33:28 MR. McKENZIE: I'm a man of my word, Your Honor. I
04:33:30 will pause questioning until tomorrow.

04:33:32 THE COURT: Let the record reflect that.

04:33:34 (Proceedings reported but not transcribed.)

CERTIFICATE OF REPORTER

I, Mary A. Schweinhagen, Federal Official Realtime Court Reporter, in and for the United States District Court for the Southern District of Ohio, do hereby certify that pursuant to Section 753, Title 28, United States Code that the foregoing is a true and correct transcript of the stenographically reported proceedings held in the above-entitled matter and that the transcript page format is in conformance with the regulations of the Judicial Conference of the United States.

s/Mary A. Schweinhagen

___________________________________ 15th of December, 2021

MARY A. SCHWEINHAGEN, RDR, CRR
FEDERAL OFFICIAL COURT REPORTER